REMARKS/ARGUMENTS

Claims 1, 3-8, 10-14, and 16-22 pending. Claims 1, 3-8, 10-14, 16-22 have been amended. Claims 2, 9, and 15 have been canceled without prejudice and without disclaimer. No new matter has been introduced thereby. Applicants respectfully submit that the claims as amended comply with 35 U.S.C. § 112.

Claims 1-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sampath et al. (U.S. Patent No. 6,266,774) in view of Kamath et al. (U.S. Patent No. 6,754,696). The Examiner states that Sampath et al. discloses the claimed invention except for the feature of a server including a storage device that is managed by the client. The Examiner cites Kamath et al. for allegedly supplying the missing teaching.

Applicants respectfully submit that independent claims 1, 8, 14, 21, and 22 are patentable over Sampath et al. and Kamath et al. because, for instance, they do not teach or suggest that:

(1) the clients do not include a local disk device; and

(2) the storage apparatus includes a program configured to update security information of clients regardless of whether or not clients are initiated.

In the present invention, security information to which clients refer is stored in a storage apparatus on the server side, and the security information is updated without a request from the clients. The clients do not include a local hard disk device (see, e.g., page 7, lines 22-23).

When the diskless client is turned on, an IPL (Initial Program Loader) is started up. A basic OS is called up from the disk images of the server through the network by the action of the IPL, and the basic OS is deployed in the memory of the diskless client (see, e.g., page 10, lines 11-16).

In a case where an application program is operated by the diskless client, when the application program requests access to a file within the disk images of the server under control of the OS, additional file access control by the security software occurs. A policy file within the disk images of the server is referenced by the file access control, and the policy is

authenticated with regard to the file(s) whose access has been requested (see, e.g., page 11, lines 5-25). Regardless of whether of not operation of the client is stopped, the policy (security information) can be updated as needed (see, e.g., page 12, lines 20-21).

Therefore, it is possible to overcome the disadvantage of the scheme of updating the security information on the client side that the client is unable to execute the access control and virus protection in an up-to-date state. This disadvantage is also discussed in the description of the related art of the present application.

In contrast, the combination of the references does not teach or suggest that (1) the clients do not include a local disk device; and (2) the storage apparatus includes a program configured to update security information of clients regardless of whether or not clients are initiated, as recited in independent claims 1, 8, 14, 21, and 22.

Sampath et al. discloses that a user computer is equipped with a storage device such as a disk drive. See, e.g., column 5, lines 8-10. In addition, Kamath et al. discloses that client devices 80 include an XFS-Client portion 33, which includes a virtual local drive 34. On the contrary, the present invention describes that the clients do not include a local disk device.

Sampath et al. discloses a method of updating software (an anti-virus program) of a client. According to this method, in response to a request from the client, a Web page is created on the server side and client authentication is performed. After the authentication is complete, a program (ActiveX) that checks software on the client side is sent from the server to the client, and it is checked whether the software of the client is the latest. If not the latest, the latest software is downloaded from the server to the client of software upgrading is performed. See, e.g., column 6, line 44 to column 7, line 43.

Since Sampath et al. discloses to update the anti-virus program after downloading it from the server computer (see, e.g., column 7, lines 30-43), Sampath et al. fails to disclose or teach the feature of the present invention that is to bring the clients' security information up to date regardless of whether or not the clients are initiated on the storage apparatus side.

In addition, the feature of Sampath has the disadvantage that the client is unable to execute the access control and virus protection in an up-to-date state until the client downloads and updates the executable program, as described in the description of the related art in the present application. Thus, Sampath et al. merely discloses the conventional art as discussed in the description of the related art of the present application.

Kamath et al. discloses a file system (called Extended File System) which enables access to files stored in a remote storage like access to a local file stored in the storage of a client, but it does not cure the deficiencies of Sampath et al., in that is also fails to teach or suggest the features described above regarding independent claims 1, 8, 14, 21, and 22.

As discussed above, an anti-virus program is downloaded or upgraded in response to a request from the client in Sampath et al. Thus, in order to update an anti-virus program, the client has been initiated. In Kamath et al., a remote file is updated as a corresponding local file is updated. That is, if the local file is updated, the file is sent to the remote and the remote file is updated to the file. Thus, when the remote file is updated, the client needs to be initiated. Sampath et al. and Kamath et al. do not suggest updating security information of clients regardless of whether or not clients are initiated.

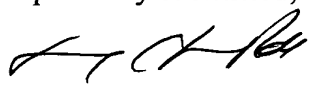
Accordingly, even if combined, Sampath et al. and Kamath et al. do not disclose or suggest that (1) the clients do not include a local disk device; and (2) the storage apparatus includes a program configured to update security information of clients regardless of whether or not clients are initiated. For at least the foregoing reasons, independent claims 1, 8, 14, 21, and 22 and claims 3-7, 10-13, 16-20 depending therefrom, are patentable over Sampath et al. and Kamath et al.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



Chun-Pok Leung
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
RL:cl
60766574 v1